SYSTEM AND METHOD FOR NETWORK INTRUSION DETECTION ANALYSIS WITH DIRECT PROTOCOL STACK MONITORING

Abstract

A system and method for detecting network intrusions using a protocol stack multiplexor is described. A network protocol stack includes a plurality of hierarchically structured protocol layers. Each such protocol layer includes a read queue and a write queue for staging transitory data packets and a set of procedures for processing the transitory data packets in accordance with the associated protocol. A protocol stack multiplexor is interfaced directly to at least one such protocol layer through a set of redirected pointers to the processing procedures of the interfaced protocol layer. A data packet collector references at least one of the read queue and the write queue for the associated protocol layer. A data packet exchanger communicates a memory reference to each transitory data packet from the referenced at least one of the read queue and the write queue for the associated protocol layer. An analysis module receives the communicated memory reference and performs intrusion detection based thereon.